FILED

MAY 08 2018

PATRICK KEANEY
Clerk, U.S. District Court
By _____ Deputy Clerk

EDOK - Application for Search Warrant (Revised 5/13)

United States District Court

EASTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF
(1) ADATA UV 128/8GB FLASH DRIVE

CURRENTLY LOCATED AT U.S. Secret Service, 520 Denison Ave., Muskogee, Oklahoma

Case No. MJ-18-073-KEW

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the **EASTERN** District of **OKLAHOMA** *(identify the person or describe property to be searched and give its location)*:

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Section(s) 1028(a)(1) and 1029, and the application is based on these facts:

☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

FRANK M. COFFMAN
Special Agent, United States Secret Service

Sworn to before me and signed in my presence.

Date: May 8, 2018

Judge's signature

City and state: Muskogee, Oklahoma

KIMBERLY E. WEST
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF (1) **ADATA UV 128/8GB FLASH DRIVE** CURRENTLY LOCATED AT U.S. Secret Service, 520 Denison Ave., Muskogee, Oklahoma.	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, **Frank M. Coffman** being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of devices described as:

a. **ADATA UV 128/8GB FLASH DRIVE, (Hereinafter "Device 1");**

for items described in Attachment B. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B. **Device 1** as described above and in Attachment A, is currently in possession of the U.S. Secret Service, 520 Denison Ave., Muskogee, Oklahoma, within the Eastern District of Oklahoma.

2. I am a Special Agent with the U.S. Secret Service, and have been since December 1998. I received training on the investigation of Counterfeit (CFT) Access Device Fraud and Identity Theft at the Federal Law Enforcement Training Center in Brunswick, GA, as well as

specialized instruction on how to conduct investigations at the Secret Service Training Academy in Beltsville, MD. I have also received additional training through continuing education training seminars sponsored by the United States Secret Service and other law enforcement agencies. I have conducted and/or assisted in numerous investigations regarding CFT Access Device Fraud and Identity Theft, conducted and/or assisted in countless interviews of witnesses and suspects involved in these investigations, and have testified in state and federal court regarding said investigations. I have also requested and received warrants to search and seize property in connection with the referenced investigations. I am also aware it is a violation of Title 18, United States Code, Section 1028(a)(1) to commit Aggravated Identity Theft and a violation of Title 18, United States Code, Section 1029 to commit Access Device Fraud and/or Conspire to do so.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. Beginning in January 2018, victims reported to Lighthorse Police Department (LPD) their credit/debit card account numbers were used at the World Winstar Casino (Winstar) in Thackerville, Oklahoma, which is located within the Eastern District of Oklahoma. Victims reported they had possession of their credit/debit cards but someone was making unauthorized cash withdrawals from their accounts. LPD is currently investigating the circumstances involving the unauthorized transactions. Via video surveillance and financial transaction reports they were able to identify several suspects involved in the crime. Investigators were able to determine that multiple fraudulent credit/debit cards were being used to access Automated Teller Machines

(ATM's) at the Winstar Casino wherein the suspects would obtain vouchers through the ATM's to either gamble or present to the casino cashier in return for cash.

5. On March 27, 2018, Sergeant Michael Huff (LPD), was working at the Chickasaw Border Casino (Border), Thackerville, Oklahoma, located within the Eastern District of Oklahoma. Sgt. Huff, who was familiar with the ongoing fraudulent credit/debit card investigation, was in the surveillance room of the casino watching a subject make several transactions with multiple credit/debit cards on an ATM. Sgt. Huff contacted Investigator (INV) Keaton Alexander (LPD) who is currently investigating numerous complaints of stolen credit/debit cards being used in the casinos of the Chickasaw Nation. Sgt. Huff texted a picture of the subject making the suspected fraudulent credit/debit card transactions to INV Alexander who recognized the subject as **Raudy Acosta Fernandez (R. Fernandez)**, a suspect in the fraud ring that INV Alexander had been investigating and following on Facebook. (On March 21, 2018, **R. Fernandez** was observed on video surveillance using multiple credit/debit cards at four different ATMs inside the Winstar Casino. INV Alexander identified **R. Fernandez** on the video surveillance from his pictures on Facebook. **R. Fernandez's** actions at the four separate ATMs using multiple cards are consistent with access device fraud.)

6. Sgt. Huff attempted to arrest **R. Fernandez** but during the course of the arrest **R. Fernandez** escaped while wearing handcuffs. INV Alexander arrived at the scene after the escape of **R. Fernandez** and saw Sgt. Huff speaking with a female subject, later identified as **Lianet Cabrera Diaz (L. Diaz)**. **L. Diaz** was standing next to a black Mercedes Benz with a temporary Texas Tag- 30C0225 (**Vehicle 2**). Sgt. Huff informed INV Alexander that **R. Fernandez** had escaped into the woods and he had previously observed **L. Diaz** in the company

of **R. Fernandez**. Sgt. Huff advised **R. Fernandez** and **L. Diaz** were seen on video surveillance arriving together at the casino in **Vehicle 2**.

7. INV Alexander asked **L. Diaz** what her business was at the Border Casino and why she was sitting on **Vehicle 2** and not inside the vehicle. **L. Diaz** responded that she was waiting on her boyfriend. **L. Diaz** did not reply when asked the name of her boyfriend. INV Alexander then informed **L. Diaz** of the incident that took place with Raudy (**R. Fernandez**) and INV Alexander asked **L. Diaz** if that was her boyfriend. **L. Diaz** acted as if she did not know Raudy. **L. Diaz** was then shown a picture from Facebook of **L. Diaz** with Raudy (**R. Fernandez**). **L. Diaz** then stated that Raudy (**R. Fernandez**) was her ex-boyfriend and that she didn't know he was at the Border Casino. INV Alexander advised **L. Diaz** that surveillance video showed Raudy (**R. Fernandez**) and **L. Diaz** arriving together at the Border Casino, however, **L. Diaz** continued to deny involvement with Raudy (**R. Fernandez**). LPD K9 Officer Jeremy Stein deployed his K9 on **Vehicle 2**. The K9 alerted and a search of the vehicle was conducted. During the search, a wallet belonging to **L. Diaz** was located on the center console. The wallet contained five MasterCard Green Dot credit/debit cards with no name on them. Several of the cards resembled fraudulent credit/debit cards used in multiple fraudulent transactions at the Winstar and Border Casinos. During the inventory of **Vehicle 2**, six additional credit/debit cards were discovered in the glove compartment. On April 3, 2018, USSS Agent Lantz Stuart utilized a credit card scanner to scan the magnetic strip on all of the credit/debit cards recovered from **Vehicle 2** to determine, among other things, information that would identify the individual(s) authorized to utilize the cards to conduct transactions. The information contained on the magnetic strip of the cards belongs to eleven separate identity theft victims.

8. During the investigation of **R. Fernandez** and **L. Diaz**, INV Alexander was contacted by personnel from the Border Casino surveillance team and advised a Silver Lincoln Navigator bearing Texas Tag- KGP6200 (**Vehicle 1**), arrived at the Chickasaw Travel Stop located near the Border Casino. INV Alexander recognized the description of the Navigator as the vehicle used to transport suspects involved in fraudulent credit/debit card transactions. On March 14, 2018, video surveillance showed suspects **Iduar Acosta Fernandez (I. Fernandez) and Migual Leon Bejarano (M. Bejarano)** arrive at the Winstar Casino together in **Vehicle 1. I. Fernandez** was later identified as using a fraudulent credit /debit card, at the Winstar Casino on March 14, 2018, via video surveillance and financial transaction reports. INV Alexander went to the Chickasaw Travel Stop and observed two male subjects, later identified as **I. Fernandez** and **M. Bejarano** standing next to the ATM machine in the Chickasaw Travel Stop. INV Alexander recognized both male subjects as suspects involved in fraudulent credit/debit card transactions. INV Alexander had previously identified **I. Fernandez** and **M. Bejarano** via Facebook photos, video surveillance and financial transaction reports, using fraudulent credit/debit cards at the Winstar Casino on January 7, 2018, January 8, 2018, March 1, 2018, and March 14, 2018.

9. On March 27, 2018, **L. Diaz, I. Fernandez** and **M. Bejarano** were placed under arrest for charges involving Identity Theft, Credit Card Fraud, and Obstruction

10. An **LG Cellular Telephone, SN: 709VTXF387450, Samsung Galaxy Note 8 Cellular Telephone, SN: 358510081626018** and **Samsung Galaxy Note 8 Cellular Telephone, SN: 358510081613297** were seized from **I. Fernandez** and **M. Bejarano** at the time of their arrest. INV Alexander advised one of telephones began receiving incoming telephone calls with

the name "Raudy" displaying on the screen which was the same name of the suspect who escaped custody. INV Alexander conducted a telephone number search through the TransUnion-TLOxp and confirmed the telephone number belonged to **Raudy Acosta Fernandez**.

11. **Vehicle 1** in which **I. Fernandez** and **M. Bejarano** arrived at the Winstar Casino was towed from Chickasaw Property. Prior to towing, a vehicle inventory was conducted wherein multiple items were discovered which are believed to be tools used to place credit/debit card skimmers on gas pumps: (1) a cordless drill with an extended phillips head bit located in the center console; (2) a pair of electrical pliers located in the center console; (3) a small pry bar located between the center console and front passenger seat; and (4) multiple latex gloves were found in the back floor board. By placing a credit/debit card skimmer on a gas pump, an individual is able to steal/obtain information from the credit/debit card inserted at the gas pump for payment that allows the individual to produce a fraudulent credit/debit card for use in illegally obtaining money or merchandise with the fraudulent credit/debit card. This type of fraudulent credit/debit card was being used by the subjects in the fraud investigations involving the Winstar and Border Casinos as referenced in this Affidavit and similar to the fraudulent credit/debit cards used by **R. Fernandez** on March 21, 2018, at the four separate ATM's, and the card used by **R. Ferndanez** on March 27, 2018, and the fraudulent debit/credit cards found in **L. Diaz's** wallet.

12. **Device 1** is currently in the lawful possession of the U.S. Secret Service. It came into U.S. Secret Service possession in the following way. On April 23, 2018, the Honorable Steven P. Shreder, U.S. Magistrate Judge, Eastern District Of Oklahoma, signed a Search and Seizure Warrant for **(Vehicle 2) 2010 Mercedes Benz, Temporary Texas Tag Number:**

30C0225, VIN: WDDHF8HB4AA103963. On April 25, 2018, the Search Warrant was executed on **Vehicle 2** located at McGehee Wrecker Service, 6476 OK-32, Marietta, Oklahoma, located within the Eastern District of Oklahoma. **Device 1** was recovered from the glove compartment of the vehicle.

13. In my training and experience, I know that **Device 1** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as it was when the device first came into the possession of the U.S. Secret Service.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. **Device 1** is an example of "storage medium" and, specifically, a "flash drive" which is a small piece of equipment that can be connected to a computer or other electronic equipment to copy and store information.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

15. As described above and in Attachment B, this application seeks permission to search for records that might be found on **Device 1**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage

media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

16. *Probable cause.* I submit that, due to the fact that **Device 1**, storage medium, was found in **Vehicle 2**, there is probable cause to believe those records will be stored on that storage medium, for at least the following reasons:

a. Based on my knowledge, past investigations, and the current investigation involving Aggravated Identify Theft and Access Device Fraud and/or Conspiracy, I know that individuals involved in said criminal activity often keep items described in Attachment B on devices like **Device 1** to facilitate and conduct said criminal activity.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on **Device 1** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when,

where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and

have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying information on storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

I submit that this affidavit supports probable cause for a warrant to search **Device 1** described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

FRANK M. COFFMAN
Special Agent
UNITED STATES SECRET SERVICE

Subscribed and sworn to before me
on May 8, 2018:

KIMBERLY E. WEST
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is:

(1) ADATA UV 128/8GB FLASH DRIVE, (Hereinafter "**Device 1**");

The Device is currently located at the U.S. Secret Service, 520 Denison Ave., Muskogee, Oklahoma.

This warrant authorizes the forensic examination of **Device 1** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on **Device 1** described in Attachment A that relate to violations of Title 18, United States Code, Section 1028(a)(1), Aggravated Identity Theft; and Title 18, United States Code, Section 1029 Access Device Fraud and/or Conspiracy, including:

a. Records, receipts, notes, ledgers, and other documents related to the manufacturing and possession of counterfeit access devices and identity theft;

b. any contact/address books, sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet, related to the manufacturing and possession of counterfeit access devices and identity theft;

c. Stored communications which are voice recordings/messages, text messages (SMS) and multimedia messages (MMS), emails and attachments, read or unread which relate to and provide evidence of the above described criminal activity and as further described in this affidavit;

d. Internet World Wide Web (WWW) browser files including browser history, browser cache, browser favorites, auto-complete form history and stored passwords;

e. any information related to sources of counterfeit access devices and identity theft (including names, addresses, phone numbers, or any other identifying information);

f. any information recording schedules or travel;

g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned **Device 1** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.